

REMARKS/ARGUMENTS

Claims 1-45 are pending in the present application. A Preliminary Amendment filed August 5, 2003, which added claims 28-45, crossed in the mail with the current Office Action. Consequently, newly added claims 28-45 were not examined by the Examiner. In the present amendment, Claims 1-2 and 12-14 were amended, and claims 20-27 were canceled.

Consequently, claims 1-19 and 28-45 remain pending.

The Examiner rejected claims 1-24, 26 under 35 U.S.C. §102 as being anticipated by U.S. Patent No. 5,778,071 issued to Caputo et al. The Examiner also rejected claims 25 and 27 under 35 U.S.C. §103 as being obvious. However, claims 25 and 27 have been canceled. With respect to the §102 rejection, it is respectfully submitted that Caputo fails to disclose each and every claim element of the claimed invention.

The present invention provides an authorization system in which a portable security device is removably coupled to a computer system to selectively authorize the use of computer programs on the host computer. The portable security device stores multiple items of authorization information that are used by the computer system to use the protected software programs and data. The portable security device includes a communication interface for communicating with multiple information authorities, such as software vendors, for downloading the authorization information to the portable security device for subsequent authorization of the vendor's software or data. The authorization information is then stored within a memory in the portable security device. In one embodiment, the type of authorization information stored in the portable security device includes secret keys, or dynamic key selectors for generating secret keys. The dynamic key selectors may be stored in encrypted form in the portable security device. Each item of authorization information stored in the device corresponds to a particular protected

software program and is used to authorize use of only that program.

When the user wishes to authorize use a protected program on the host computer, the user connects the portable security device to the computer system, using a USB port, for instance. The host computer initiates a challenge-response transaction with the portable security device to determine whether the security device contains the proper authorization information for the protected software program. The challenge message transmitted to the security device includes a key ID identifying the protected software program. In response, the security device retrieves the dynamic key selector corresponding to the key ID, decrypts the dynamic key selector, and generates a secret key from the dynamic key selector. The portable security device then transmits a response message to host computer that is a combination of the challenge message and the generated secret key. The secret key in the response then authorizes the host computer to access the protected software program.

Referring now to the claims, independent claims 1, 2, 12, and 14 have been amended to recite that the protected information “includes software,” and that the first and second items of authorization information are “associated” with first and second items of protected information, respectively. Claims 1, 2, 12, and 14 have further been amended to recite that the first and second items of protected information are “provided by a vendor.” Support for these amendments may be found throughout the Specification, such on pages 7-10 for example. The claims have also been amended to recite that the host is selectively authorized to use the items of protected information based on the first or second items of authorization information “being stored therein”. Support for this amendment may be found in the Specification on page 5 lines 25-27, for example. Previously added independent claims 28, 32, and 36 include similar recitations.

In contrast to the present invention, Caputo is directed to a portable security device having a network communications interface that provides encryption and authentication capabilities to protect data and restrict access to authorized users (col. 1, lines 10-15). The device integrates security and interface functions to be used as an access control means to another computer or network (col. 3, lines 39-43). The portable device can be used as an identifying token, a communications network interface, a data encryptor, and a user, device and/or message authenticator. It provides an electronic token which can be carried by the user to quickly identify him or her to a network, to a computer system, or to an application program. The device contains a modem for connecting the device to a data transfer path, such as a telephone network (column 5, lines 7-15). A PIN identifying the user is entered into the device either by a keypad or a smartcard (col. 2, lines 23 – col. 3, lines 15). The device will not permit communications to proceed until the device and optionally, the user, have been identified by the authenticator. The device also contains all of the cryptography required to protect the data using data encryption or message authentication or digital signatures or any combination thereof (column 5, lines 15-27).

The device of the present invention and the device of Caputo have different purposes. The device of the present invention is intended for copy-protection of digital information (including software) on a computer, whereas Caputo's device protects access to information on a network by a particular device or user. These different purposes have led to different methods of protection.

The method that Caputo uses for protecting access to information is identification of the device or the user. If servers on a network can verify the single identity of the device and/or the user, then access is granted. Caputo's device does not have the intelligence to determine what multiple pieces of information on the computer the user is allowed to access or not. Access is

ultimately controlled by the servers on the computer network.

This is contrasted by the device of the present invention, which alone selectively controls access to protected pieces of information on the computer based on authorization information associated with the protected items that are stored in the device. For example, authorization #1 must be present in the device in order to gain access to information item #1 on the computer; authorization #2 must be present in the device in order to gain access to information item #2; etc. The device can hold many of these authorizations to allow access of many items of information. The identity of the device or the identity its user in no way plays a role in determining access to pieces of information. In addition, a server and/or a network are not needed for the device of the present invention to grant access to the computer to use the protected information.

As Caputo discloses a device for protecting access to information through device/user identification, Caputo fails to teach or suggest the claimed invention, which authorizes the use of “software” and data on a computer, as claimed.

Insofar as Caputo’s device is for protecting access to information through device/user identification and requires different methods/functionality to achieve that purpose, Caputo’s device fails to solve the problem solved by the present invention, which is how to authorize the use of “software” and data on a computer in a manner that even an authorized user cannot make usable copies of the information being protected for an unauthorized user.

Although Caputo teaches the use of well-known PINS, and encryption and decryption keys that are kept secret, the PINS and keys are not “associated” with data or programs on the computer system. Therefore, Caputo also fails to teach or suggest a device that can receive “first” and “second items of information,” each respectively “associated” with first and second items of

protected information, which are provided by a “vendor,” as recited in claims 1, 2 and 12-14.

Likewise Caputo fails to teach or suggest a device that receives "multiple items of authorization information (such as key selectors) associated with the multiple items of protected information," and then authorize the computer to use one of the items of protected information "based upon the corresponding item of authorization information" stored in the memory," as recited in claims 28, 32, and 36.

Caputo also fails to teach or suggest a portable security device for selectively “authorizing” the host system to use the *one or more items of protected information* based upon the first or second items of authorization information being stored therein,” as recited in claim 1, or for "selectively authorizing the computer system to use multiple items of protected information" to be executed on the computer system, as recited in claim 28.

With respect to independent claim 14, the arguments above apply with full force and effect. In addition, claim 14 specifically recites “key selectors,” the function of which are neither taught or suggested by Caputo because Caputo’s PINs are not “associated with a first one of the items of protected information and provided by a vendor of the first one of the items of protected information,” as claimed.

With respect to claims 16-19, it is respectfully submitted that Caputo fails to teach or suggest a portable device that stores "one or items of blended authorization information that are “derived from a plurality of items of authorization information.” As stated above, Caputo's PINS fail to provide the same function as the claimed items of authorization information. In addition, it is believed that Caputo's device does not store multiple PINS therein, not to mention blending multiple ones of the PINS together.

To the extent that the claims of the present invention recite “encryption,” it is noted that

the Caputo device uses encryption/decryption on the information being protected. However, the purpose of Caputo's encryption is to prevent the interception of sensitive data as it travels over the network. In contrast, the device of the present invention does not encrypt/decrypt information that is protected and authorized. Instead, the protected information is stored on the computer awaiting authorization. Because the method and purpose of the device of the present invention are different from those of the Caputo device, this functionality is not needed in the present invention.

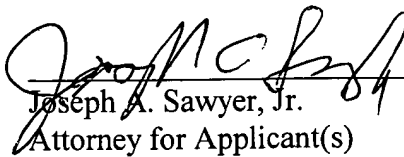
In view of the foregoing, it is submitted that claims 1-19 and 28-45 are allowable over the cited references. Accordingly, Applicant respectfully requests reconsideration and passage to issue of claims 1-19 and 28-45 as now presented.

Applicants' attorney believes that this Application is in condition for allowance. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Respectfully submitted,

SAWYER LAW GROUP LLP

February 6, 2004
Date


Joseph A. Sawyer, Jr.
Attorney for Applicant(s)
Reg. No. 30,801
(650) 493-4540